資料2

高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議
企業・個人評価指標専門委員会
第１回会合議事要旨

１．日　時

平成 18 年８月３日（木）　14 時 00 分～16 時 00 分

２．場　所

内閣府別館会議室

３．出席者

【委　員】

井上　克至　委員（エヌ・ティ・ティ・データ・セキュリティ株式会社取締役）
大木　栄二郎　委員（工学院大学教授）
佐々木　良一　委員（東京電機大学教授）
下村　正洋　委員（ＮＰＯ日本ネットワークセキュリティ協会事務局長／株式会社ディアイティ代表取締役社長）
田辺　国昭　委員（東京大学教授）
中尾　康二　委員（KDDI㈱技術開発本部情報セキュリティ技術部長）
滑川　恵理子　委員（㈱サンケイリビング新聞社マーケティング戦略室編集企画部長）
牧野　二郎　委員（弁護士）
村上　輝康　委員（㈱野村総合研究所理事長）

（五十音順）

【政　府】

内閣官房情報セキュリティセンター長
内閣官房情報セキュリティセンター副センター長
内閣官房情報セキュリティセンター情報セキュリティ補佐官
内閣官房情報セキュリティセンター内閣参事官
警察庁生活安全局情報技術犯罪対策課長
防衛庁運用企画局情報通信・研究課情報保証室長
総務省情報通信政策局情報通信政策課情報セキュリティ対策室長
文部科学省大臣官房政策課情報化推進室長
経済産業省商務情報政策局情報セキュリティ政策室長

４．議事要旨

(1)　各委員の紹介と委員長の選出

○　村上委員を委員長に選出

(2)　村上委員長挨拶

(3)　会議の公開等について
○　事務局より説明、原案のとおり了承

(4)　企業・個人評価指標専門委員会の位置付けについて
○　事務局より説明

(5)　我が国政府の情報セキュリティ問題への取り組みについて
○　事務局より説明

(6)　企業・個人の情報セキュリティのあり方
－企業・個人評価指標専門委員会の出発点－
○　事務局より説明

(7)　各委員の意見開陳
○　情報セキュリティの取組みについて、PDCA との関係では、Ｐは基本戦略という形でまとまっており、Ｄもセキュアジャパン 2006 というのが具体的な姿になっている。しかし、これをＣでチェックをして、アクションにつないでゆくためのチップがない。このＣのところをつくらなければならない、ということだろうと。
そのポイントは、意識面・対策面・結果面という三つの側面であると考えている。

○　最終的に情報セキュリティというものが実際に達成されているかというのは、まさしく行動に表れているかどうかというところだと考えている。
また、意識面の測定というのは非常に難しいだろうと思っている。心理学的な側面も入ってくるため、一筋縄では行かない。

○　外形的に分かるところを計測し、評価するしかないと思う。

○　企業・個人が 2009 年の始めに到達するべき姿については、何らかのモデルが必要である。そして、何がこのモデルたり得るかというと、大企業にとっては政府機関がやろうとしていることが、中小企業にとっては地方公共団体がやろうとしていることがモデルではないか。政府職員の育成も企業の人材育成の参考となろう。
そういう意味で言うと、政府機関等に係る話と表裏一体ですすめていかないと、難しいのではないか。

○　結果の評価は、何らかの客観的な評価ができるのだと思うが、過程については、様々なファクターがあるので、結果と施策の関係の評価は、構造解析でもしない

限り難しいと思う。

○　定量的にみてゆこうとした場合、まず、データがないといけないが、データ収集には予算上の制約がある。データと政府の施策とのつながりの把握も非常に難しい。

○　個人と企業、企業と個人の関係について。感じとしては、森をみて、綺麗な森だったらよいということだと思うが、その綺麗な森とは何か。その中には木があって草があって、生き物がいて、大きな木が綺麗に並んでいるのがよい森なのか、里山のようないろんな植生のほうが、それがよい森なのか。そういったことを議論してから入っていかないといけない。そうしないと、すごく綺麗な、植林された杉林の直線的な森になってしまう。

○　考えるに、何らかのモデルが必要。ただし、先ほどの森の例で言うならば、森のモデルではなく一個一個の植生のモデル。

　モデルとして注目しているのは、政府機関の統一基準。あれがどのようにつくられ、どのように実施され、どのように評価され、またそれをどのようにつくるのかということ。

　それを社会が見ながら動いていくと思っている。

○　無理な尺度、無理な評価基準をつくらないようにしなければならない。例えば、資本金１億円の会社が 1000 万円のセキュリティポリシーを実際にかけられるかなど。

○　大企業と中小企業を考慮したとき、一律的な情報セキュリティの要求は不可能かもしれない。

○　セキュリティは政府による公共財の性格を有しているといえる。そのため、その評価については、国防や安全の評価をどういう指標で測定するのかという問題と同じような形で検討する必要がある。

○　セキュリティの評価指標は、おそらく外部性を持っている。例えば、個人については、何をやったからどう評価されるというものではなく、他人がどの位やっているのかとの比較で評価が決まってくる。

　そのことは、評価指標をつくる際に難しい問題となる。

○　企業のところで、出したがらないセキュリティに関する情報をどう出させるのかという問題がある。

　情報を集めるコストをどのように考えてゆくのか、というのも今後指標設定等で考えていかなければならない。

○　究極の安全というのは、ある程度不安を何も感じてないところで上手く動いているという世界だと思う。情報セキュリティというのがきちんと意識されているというのは、ある意味でやばいと思っているからみんな意識している。これをど

う考えるかということは、ある意味ではセキュリティの全体のイメージにかかってくるのではないか。

○　対策面については、施策がどの程度進んでいるのかをチェックすることになるが、ここのところは今までの制度の蓄積があるので、できるのではないかと思う。

○　結果面に関しては、社会指標をどうつくるのか、というような問題になってくるのではないか。

○　この分野では、技術と環境の持っている影響力が圧倒的であると思う。例えば、今年度評価指標をつくって、2006 年度の評価では大丈夫だとしても、来年はもしかしたら回答が違ってくる。ベンチマークを変えてゆく、あるいはフレキシブルに対応するということを指標の中にも全体のイメージの中にも取り込んでいくのが良いのではないか。

○　いろいろな課題についていろいろ考えて行くと、２年以上かかる話であり、２ケ月では無理。むしろ段階的スケジュールを考えていくべきであろう。

○　直感的な印象として、たたき台がないとなかなか議論はできないと思うし、企業と個人、この二つを同一のテーブル上で議論するのは困難である。共通部分もあるが、少しわけて議論することもあるのではないか。
　たたき台として考えられるものとして、政府の統一基準があげられるかもしれないが、それで企業・個人を考えたときには、若干ずれがあるのではないか。

○　評価指標というのは、最初は当然政府の政策が本当にうまく言っているのかというレベルを考えるのかもしれないが、例えば各企業・個人を対象としたときのセキュリティの成熟度を考えたときに、それをどういうふうにはかってゆくのか、ということも言えるかもしれない。

○　いろいろな観点から、あるレベルでたたき台をつくっていただき、企業・個人、どのように分けるかはわからないが、精力的に進めて行ければと思う。

○　レベルも年齢もまちまちという現在のインターネットの利用者の状況を考えると、外から測るのは難しいのではないかと思う。

○　この問題を難しいものとしているのは、見えないものを見えるようにしなければならないからではないか。具体案を書かない限りは絶対に前に進まないだろう。

○　今回は、大胆に案を決めてしまわないと前に進まないのではないかと思っている。

○　セキュリティの基準については、絶対基準というよりは、どちらかといえば相対基準に近い考え方であると思う。

○　この委員会で、荒削りでも良いから、企業規模を４つくらいにわけて、それぞ

れの具体的な達成基準と達成時期をたたき台としていくつかつくってみて、それをみんなで徹底的に叩いてみる、ということが必要ではないか。

○　評価対象を結果論としてどう見るのか、不正アクセスの被害が減ったからよいのか、という議論については、やはり相当な暗数が存在するので、そう簡単には見えないと思う。

(8)　自由討議

○　例えば東証のシステム問題などはセキュリティの問題なのか、それともシステムの問題なのか、というのがわからない。

むしろ、企業の内部統制的には、その事業計画が杜撰であったということが一番最初にあるのではないか。すなわち、事業計画と情報システムとの問題として考えたのち、最後に、情報セキュリティの問題として考えてゆくのではないか。

土俵をきりわけるか、それとも情報システム、安全なサービスまで考えてしまうか。その辺をきちんと決めないと、議論が散漫になってしまうのではないか。

○　対象がいろいろと広まったり狭まったりすることもあるため、今のところは余り限定しないでやっていった方が生産的。

なお、東証の問題も全くセキュリティの問題外であるとは言えない。システムの成熟度が低いものが存在すること自体も、やはりセキュリティの問題であると思う。

最後には綺麗な定義ができるかもしれないが、とりあえずは「情報セキュリティのようなもの」というところを対象として、できるだけまずは広く見てゆく

○　二ヶ月でやる以上、中味の「粗さ」について意志統一しておかないと、限られた時間の中でやって行くのは難しいのではないか。

○　先ほど、下敷きにできるものとして、政府としては統一基準、企業としてはISMSがあるということだったが、両方とも詳細なものである。

そこで、企業規模毎に分類した４つのモデルを議論の出発点にするか、あるいはもう少しトップダウンで2009年のあるべき姿を議論して、そこからスタートすべきなのか。アプローチの方法として大きな分かれ目となる。

○　資料５の10頁のところで企業のレベルを三つにわけているが、恐らく、昨年春に経産省が作成した情報セキュリティガバナンスの報告書などを見て分類したものと思われる。

これは、事業構造上の脆弱性と社会的影響力を勘案して三つのレベルに分けたのであるが、例えば、前年まで一般企業としか取引をしていなかった中小企業が、次の年には国家機密に関わる業務に携わる等、ある企業に求められるレベルは時とともに変化する。つまり、規模等で企業の位置を固定的に分類することは不可能である。

○　具体的なたたき台をつくるときに、チェックリストを作成することになると思うが、企業については、例えば ISMS というのが、情報セキュリティというものをある程度定義している。
　ISMS を一つの参考にするのであれば、目的レベルで 33 あるが、33 というのは案外大きな枠でくくっているので、その中の一つ一つを洗っていただき、指標を洗い出すための軸にするのは、一つの取りかかりとしてはよいのではないかと思う。

○　今回の評価については、外側に対するサービスの安全性といった指標も組み込まなければならないような気がする。

○　ゼロから出発しては結論にたどり着けないので、やはり ISMS とかから議論せざるを得ない。

○　企業向けと個人向け、二つに分けてモデルを明確にする必要があるのではないか。

○　現状を示す指標、いわゆるプライベートセクタにおける対策、それに対する国とか政府の施策、現象として表れるもの。それが人にどういう形で影響を与えるのかなどを絵にした上で、それと目的を対応させ、今どこを議論しているのかについてある程度合意をとらないと、この手の議論はかみ合わなくなることがあるので、合意は是非必要である。

○　個人と企業の情報セキュリティの模様を測るということであるならば、予防策の浸透度合いとか結果、つまり情報漏洩がおこっているかとか、情報事故が起こっているかということを調べて、それを突き合わせ、その相関をみてゆけば良いという議論と、対策レベルまで入り、望むべき対策を決めなければ指標ができないのではないかという議論がいったり来たりしている。まずそこをはっきり決めてしまう必要があるのではないか。

○　いずれにせよ、期間を決めて議論してゆかなければならないと考えている。
　その結果がある程度持てばよいが、多分持たないだろう。

○　最初に二つ目的があるように感じた。一つは現状を把握し、世界トップクラスの水準にあるのかどうかを判断する。もう一つは、そこにいたる政策、現状に至る政策として何が効いたのかも見なくてはならない。
　つまり、それがわかるような仕組みが必要だと。

○　いろいろ委員会をやっているなかで、望むべき対策のモデルの検討をしている場所があるのならよいが、ないのであれば、それをやらざるを得ないのではないか。

○　評価専門分科会で行ったモデル化の手法が、結構難しいが参考になるのではないか。

○　2009 年の姿については、世界トップクラスの水準の対策をする、不安を感じる個人がゼロになる、という姿しかとりあえずない。これをどのように考えればよいか。これでいきなりスタートすることはできないので、もう少し具体的なものがあれば、目標水準の議論には有用ではないか。

○　トップクラスの水準にするということは、ある種相対的な目標だが、とすれば世界の水準がわからないとどの位置にあるかがわからない。先進国の企業のセキュリティ対策がどの程度であるのか、というデータを調べなければならない。

○　恐らく、本当に指標が定まって国際比較しようとするときには、二ヶ月というようなタイムスパンではないスパンできちんと調べなくてはならない。とすれば、国際比較は難しいのではないか。

○　事務局としては、今回は国際比較までは踏み込みきれないと思っている。入れればよいが。

○　先ほど、政府がモデルではないかとの話があったが、本当に政府はベストプラクティスになっているモデルとしてもよいのか。

○　企業から見ると、それでも政府がモデルだと思う。
　政府がモデルではないということになると、企業は何をもって判断することになるのか。

○　小規模の企業と、大規模の企業と、中規模の企業で一般顧客を対象とする取引を行っているか否かで幾つかグルーピングして、それぞれ考えなければならないのではないか。

○　企業が今何を悩んでいるかというと、情報セキュリティは金がかかるが、どこまでやったらよいのかさっぱりわからない。ある一定の体制整備とか、何ランクかにわけてこういうふうにやったらどうかと、場合によっては「適」マークみたいなものが出来てくるようになれば良いのではないかと。

○　企業は、それぞれが頑張るという形で実際には進んでいるので、一つの方向としてはそれで推進し、結果として何年かして見たときに、結構世界のトップクラスを走っているという評価になるのではないか。
　そういう意味では、「世界一」という指標の取り方もよくわからないので、基準ではないのではないか。

○　この委員会は目標の設定をする場なのか。企業は誰かが言ってくれるのを待っているので、やることには賛成だが、二ヶ月でできるとは全然思えない。

○　先ほどから目標の話が出ているが、昨年４月に経産省がまとめた報告書では、ブランド、売上高、社員の離職率等の 15 の指標を統計学的に分析し、階層別に求められる対策レベルを示している。これは経産省から企業に普及啓発しているだ

けではなく、政策会議で定めた政府機関統一基準においても、政府機関が委託先企業の情報セキュリティ水準の評価に応用すること等が示唆されている。つまり、議論になっている目標については、既にそういうものが存在している。

(9)今後のスケジュール説明

○　事務局から、今後のスケジュールについて説明がなされた。

(10)内閣官房情報セキュリティセンター長挨拶